11 de diciembre de 2011

Imprimir Página Web

Control biométrico: el necesario debate público (ARI)

James C. Ross

ARI Nº 154-2003 - 31.12.2003 (Traducción del inglés)

Tema: Podría decirse que los sistemas de identificación biométrica proporcionan a EEUU y a la Unión Europea la fórmula mágica para solucionar algunos problemas de seguridad clave (como el terrorismo internacional, la delincuencia organizada y la migración ilegal) asociados con la usurpación de la identidad y la falsificación de documentos. Al ir pasando la utilización de la tecnología biométrica de ser algo marginal a ser usual, han surgido importantes cuestiones de fondo en torno a la protección de datos, la privacidad de las personas y las libertades civiles.

Resumen: En respuesta a los ataques terroristas del 11 de septiembre de 2001, EEUU y la Unión Europea han adoptado soluciones de identificación biométrica destinadas a mejorar la seguridad de los documentos y ampliar las capacidades de control sobre ciudadanos extranjeros. Los sistemas biométricos se emplean para identificar, verificar y clasificar la identidad de una persona basándose en características físicas o del comportamiento almacenadas en redes informáticas. Las razones que suelen aducirse a favor de la adopción de sistemas biométricos son el control de fronteras, la protección contra la falsificación de documentos y la usurpación de la identidad, el rastreo de inmigrantes ilegales y delincuentes sospechosos y la prevención del terrorismo. Dejando de lado cuestiones técnicas sobre la fiabilidad de su funcionamiento en la práctica, las tecnologías biométricas ponen de manifiesto algunas cuestiones de fondo en torno a la protección de datos, la privacidad de las personas y las libertades civiles, que no han recibido el suficiente debate público en España y otros países de la Unión Europea. La finalidad de este análisis es servir de introducción al origen y la función de los sistemas de vigilancia y autenticación biométrica, comparar los usos actuales y propuestos de la biometría en EEUU y la UE derivadas, respectivamente, de la *Patriot Act* y del Sistema de Información de Schengen, y comentar las cuestiones de fondo que surgen de la adopción y la "armonización" generalizadas de los sistemas biométricos. Se concluye aportando algunas recomendaciones políticas de carácter general.

Análisis:

El contexto de la biometría

Se están creando nuevos modos de integración electrónicos cuya finalidad es reducir la identidad a una serie de características biológicas del cuerpo humano "inequívocas". Gracias a nuevas tecnologías de la información como los sistemas biométricos, los Estados disponen de nuevas herramientas con las que resolver gran número de problemas de seguridad. Al combinar la invisibilidad de las "fronteras virtuales" que ofrecen las redes de datos con la visibilidad del cuerpo humano, se obtienen nuevas formas de integración de datos, vigilancia pública y control social. Los Estados dirigen sus miradas hacia las soluciones biométricas para impedir que los inmigrantes ilegales, los delincuentes y los terroristas entren en sus territorios, y garantizar simultáneamente un flujo eficiente de personas, bienes y servicios a través de las fronteras internacionales.

Introducción a la biometría

Mejorar la seguridad de los documentos se ha convertido en una cuestión prioritaria para la formulación de políticas tanto en EEUU como en la UE, aunque rara es la vez que se han publicado en grandes titulares las medidas de amplio alcance aprobadas. Los sistemas de identificación biometríca se sitúan en la vanguardia de estos nuevos progresos. Las tecnologías biométricas prometen ofrecer altos niveles de seguridad gracias a sus soluciones de identificación y verificación de las personas como medida para fortalecer la defensa contra el terrorismo, la delincuencia organizada, la inmigración ilegal y la usurpación de la identidad. Los sistemas biométricos no van a reemplazar a métodos tradicionales de identificación como los documentos nacionales de identidad o las tarjetas de la seguridad social, sino que van a complementarlos, y se podría decir que a fortalecerlos. La edición de 2001 de la *MIT Technology Review* puso de manifiesto la creciente importancia de la biometría presentándola como "una de las diez tecnologías incipientes que cambiarán el mundo". Esta parte del análisis define la biometría y expone algunas de sus principales aplicaciones.

La división RAND de Seguridad Pública y Justicia define la biometría como "cualquier característica o rasgo personal automáticamente medible, sólido y distintivo que pueda emplearse para identificar o verificar la identidad de una persona" (la publicación se puede consultar en ***http://www.rand.org/publications/DB/DB396/***). Los sistemas biométricos se utilizan principalmente para identificar, verificar y clasificar la identidad de una persona basándose en características fisiológicas o del comportamiento capturadas y archivadas en redes informáticas.

En pocas palabras, cualquier muestra biometríca *susceptible de ser medida* tiene que poder recuperarse y convertirse en un

formato digital cuantificable con facilidad. La *solidez* de la muestra se evalúa mediante la capacidad de variación del material humano básico a lo largo del tiempo como resultado de la edad, heridas, enfermedades, exposición a sustancias químicas, etc. Por ejemplo, a lo largo de la vida el iris de una persona ofrece muy pocos cambios, lo que ofrece un alto grado de solidez si lo comparamos con la voz, que está sujeta a un grado mayor de variabilidad. Por otra parte, la medición de los *caracteres distintivos* se ocupa de las variaciones o diferencias que se registran en el modelo biométrico entre la población en general. En el caso de las huellas dactilares, por ejemplo, el grado de carácter distintivo es mayor, lo que las convierte en un identificador más preciso.

Por último, la biometría empleada para reconocer personas se basa en procesos de *identificación y de verificación*. Mediante la identificación, el sistema responde a la pregunta de ¿quién es X? realizando una "búsqueda comparativa" (1:N) en la que se compara una muestra biométrica con una población de registros almacenados en una base de datos. Por otro lado, los procesos de verificación preguntan "¿se trata de X?" cuando un usuario afirma ser X. Esta transacción realiza una "búsqueda individual" (1:1), mediante la cual el usuario direcciona al sistema, a la plantilla "capturada" previamente y almacenada en la base de datos. A continuación, el sistema compara la nueva muestra biométrica con la plantilla definida por el usuario con la intención de verificar la identidad de la persona X.

Las autoridades públicas y el sector privado están realizando pruebas y mejoras en el sector de la biometría; algunos ejemplos de ello son: dispositivos de barrido del iris, la retina y las huellas dactilares, sistemas de reconocimiento vocal y facial, verificación digital de la firma y dinámica de tecleo, etc. Se espera que la identificación del ADN o la "huella genética" se conviertan algún día en el identificador personal que supere a todos los demás, dada su fácil capacidad de medición, su solidez y el alto grado de individualidad que ofrece. Se espera que el ADN aporte una forma inequívoca para vincular los registros de una base de datos con personas, haciendo posible la integración y descentralización de datos. Los Estados miembros de la UE ya comparten datos de ADN capturados en sus respectivas bases de datos nacionales para combatir la delincuencia, y llevan tiempo trabajando en la creación de una base de datos europea sobre el ADN (Diario Oficial de la UE n° C 193 de 24/06/1997). Con el tiempo, la recopilación y almacenaje de ADN suscitarán gran cantidad de preocupaciones acerca de qué tipo de información personal se puede recabar a partir de muestras de ADN.

Por el momento, en opinión del US National Institute of Standards and Technology (NIST), la utilización "convencional" de la biometría para la autenticación personal se está convirtiendo rápidamente en el método que prefieren las autoridades para identificar y verificar la identidad de una persona. Entre sus numerosas aplicaciones, los sistemas de biometría prometen formas más fiables de identificar y verificar el estado de un inmigrante para seguirle mejor el rastro o restringir su acceso al país, a la percepción de subsidios y al trabajo. Además, los defensores del sector biométrico no dudan en afirmar que se podrán salvar vidas, encontrar a niños desaparecidos y detener a terroristas. También afirman que la biometría "protege la privacidad" al realizar una identificación y verificación más fiables en la lucha contra la usurpación de la identidad. En términos de operatividad, se supone que las características biométricas aportan mayor precisión en las mediciones, velocidad (tasa de tránsito), aceptación pública, resistencia a la falsificación, exigencias de almacenaje aceptables y un rápido proceso de inscripción, lo que convierten a la biometría en la solución clave para gran número de problemas de seguridad. (Si desea más información, puede consultar **www.itl.nist.gov/div895/biometrics/about.html** y también el Biometrics Consortium del Gobierno norteamericano en ***www.biometrics.org***).

Política de EEUU en torno a la biometría

En EEUU, la utilización generalizada de sistemas biométricos aplicados a la población civil se empezó a preconizar ya antes de los ataques del 11 de septiembre de 2001, principalmente a través de la ley *Illegal Immigration Reform and Immigrant Responsibility Act of 1996* (PL 104-208). La política actual de EEUU en torno a la biometría deriva de la Sec. 403 (c) de la *USA-Patriot Act* (PL 107-56) que orienta explícitamente al gobierno de EEUU hacia el "desarrollo y certificación de una norma tecnológica que pueda utilizarse para verificar la identidad de una persona" que solicita o quiere entrar en EEUU mediante un visado "con la finalidad de llevar a cabo una comprobación de sus antecedentes, confirmar su identidad y garantizar que la misma persona no haya recibido otro visado bajo un nombre distinto".

En su declaración del 12 de abril de 2002 ante el *Subcommittee on Immigration*, el Dr Arden L. Bement, Jr., director de NIST, daba cuenta de las disposiciones de esta legislación vinculadas con el desarrollo de sistemas biométricos. La ley exigía:

"Denegar el visado a aquellos extranjeros en cuyos registros apareciesen antecedentes penales o estuvieran incluidos en listas de 'vigilancia'; y verificar que la persona que solicita ser admitida en EEUU mediante un visado legítimo coincide con la persona a la que se expidió originalmente el visado… Se tiene que contemplar la necesidad básica de ofrecer una identificación precisa para garantizar que ningún terrorista será admitido en EEUU."

La finalidad de la declaración del Dr. Bement era describir los trabajos técnicos que tenía que realizar el NIST para cumplir con los objetivos de la recién aprobada ley *Enhanced Border Security and Visa Entry Reform Act* de 2002 (PL 107-173), que exige que para el 26 de octubre de 2004 únicamente se expidan visados y documentos de viaje y de entrada al país que utilicen identificadores biométricos y que sean resistentes a la falsificación y puedan ser leídos por máquinas. Además, el *Immigration and Naturalization Service* (INS) está evaluando en colaboración con el Departamento de Estado, el tipo de sistema biométrico

que se va a implantar en los controles fronterizos de EEUU para conseguir unas “fronteras inteligentes”, y acaban de anunciar planes para adoptar la biometría facial como el identificador clave para los futuros pasaportes “inteligentes”.

Para tal fin, el 5 de mayo de 2003, el Departamento de Seguridad Nacional de EEUU lanzó un programa denominado *US Visitor and Immigration Status Indication Technology* (US VISIT) cuya finalidad es asegurar las fronteras de EEUU mediante un sistema de entrada y salida automatizado. El sistema recopilará identificadores biométricos junto con fotografías digitales de todas las personas que visiten EEUU para ayudar al personal de aduanas a decidir si admiten a una persona y/o comprobar la salida de la misma. Para octubre de 2004, también se exigirá a todos los países con “exención de visado” (los actuales Estados miembros de la UE) ofrecer información biométrica a la entrada, si es que sus pasaportes no contienen todavía ningún dato de este tipo. Como voy a discutir más adelante, los enfoques de la política de la UE sobre la biometría son muy similares a los de EEUU, especialmente desde que los legisladores de ambos lados del Atlántico impulsan iniciativas destinadas a normalizar la introducción de la biometría en todos los pasaportes para un futuro no muy lejano.

Políticas de la UE en torno a la biometría
Mientras la UE busca adoptar un enfoque común para abordar problemas transnacionales como la migración, el crimen y el terrorismo, han surgido un abanico de posibilidades de aplicación de la biometría como parte integral de recientes propuestas. No obstante, la política actual se asienta sobre la imperceptible integración electrónica que implantaran los Estados miembros desde la adopción del Sistema de Información de Schengen (SIS), la “columna vertebral” del Acuerdo general para abrir las fronteras internas de la UE. El objetivo inicial del SIS era tranquilizar a los Estados miembros en el sentido de que al abrir las fronteras internas no se vería amenazada su seguridad.

El SIS empezó a ser efectivo oficialmente el 26 de marzo de 1995 y actualmente cuenta con un registro de más de 10 millones de personas. La información del sistema sigue siendo nacional, aunque el sistema en sí sea europeo. Originalmente creado para realizar el control y seguimiento de los inmigrantes y los solicitantes de asilo, el SIS archiva y proporciona datos sobre personas a las que anteriormente se ha rechazado la entrada, han sido detenidas, deportadas, se les ha denegado la solicitud de entrada o son inmigrantes ilegales, delincuentes o sospechosos de terrorismo.

A finales de 1996, como resultado de la ampliación de la UE y habida cuenta de que el sistema SIS original se estaba quedando cada vez más obsoleto, la Comisión de Schengen aprobó la sustitución de SIS por SIS II, aumentando así notablemente su capacidad e introduciendo nuevas funciones tecnológicas, en concreto la introducción generalizada de la biometría. Una propuesta española contempla que Europol, los miembros nacionales de Eurjoust y las autoridades judiciales de cada país dispongan de acceso a SIS II, y que se aumenten significativamente las funciones de consulta incluyendo nuevos tipos de personas y nuevas formas de datos. La idea es extender la utilización del SIS en la lucha contra la migración no autorizada, el tráfico de personas y el terrorismo internacional.

Tanto el SIS como el SIS II serán supervisados por organismos nacionales en materia de protección de datos, bajo los auspicios de la Directiva sobre Protección de Datos de 1995 (95/46/EC), que se refiere al procesamiento de datos personales, entre los que figuran los datos biométricos. Estos organismos nacionales estarán dotados de la autoridad para entender de reclamaciones sobre la protección de datos, investigar quejas e intervenir cuando resulte necesario. No obstante, estos organismos no cuentan actualmente con el personal suficiente para cubrir el amplio abanico de tareas que deben realizar. Como quiera que la supervisión del procesamiento de datos biométricos aumentará su carga de trabajo, será necesario dotarles de recursos adicionales [COM (2003) 558 final, 24/09/2003].

Además, se comenta que EEUU y la UE están cooperando para situarse a la vanguardia en materia de normas internacionales para la utilización de la biometría en documentos de viaje. Por el momento, una norma internacional combinaría las huellas dactilares con el reconocimiento facial biométrico para mejorar las medidas de seguridad asociadas a los viajes internacionales, la migración, los delitos y el terrorismo. Durante la reunión del G-8 del 5 de mayo de 2003 celebrada en París, los ministros de Justicia e Interior de todos los países miembros anunciaron la creación de un grupo de trabajo internacional sobre la biometría destinado a crear normas de alcance global.

En la Cumbre de la UE de junio de 2003, la Comisión Europea desveló un comunicado en el que se ponía de relieve la necesidad de un “enfoque coherente sobre los identificadores biométricos y los datos biométricos en la UE que traería como resultado soluciones armonizadas para los documentos de ciudadanos de países ajenos a la UE, pasaportes de ciudadanos de la UE y sistemas de información”. Más tarde, el 24 de septiembre de 2003, la CE publicó propuestas para la adopción de identificadores biométricos destinados a regular los visados y permisos de residencia de ciudadanos de terceros países [COM (2003) 558 final, 24/09/2003]. Estos reglamentos pendientes de ratificar mantendrían el almacenamiento obligatorio de imágenes faciales y huellas digitales como identificadores biométricos primarios y secundarios, respectivamente, de los ciudadanos de terceros países y, unos años más tarde, de todos los ciudadanos de la UE. La mayoría de estos progresos y los problemas sobre el control biométrico que llevan asociados han pasado desapercibidos para la inmensa mayoría de los ciudadanos de los Estados miembros.

Preocupaciones y recomendaciones

Las tecnologías biométricas –a pesar de sus supuestos beneficios– parecen preocupantes en lo que respecta a la protección de datos, la privacidad de las personas y las libertades civiles. En este capítulo voy a abordar algunas importantes fuentes de malestar en torno a la biométrica y voy a proponer algunas recomendaciones para los políticos españoles y los de la UE.

Las preocupaciones más alarmantes sobre la biometría proceden de sus capacidades integradas de "control de datos". Por control de datos nos referimos a la recogida de información sobre una persona identificable a partir de múltiples datos públicos y comerciales que pueden asociarse con perfiles del carácter o del comportamiento. La inspección de datos saca a relucir cuestiones críticas sobre las dimensiones clasificatorias y ampliamente discriminatorias del control biométrico. Si no se adoptan las medidas protectoras convenientes, la inspección de datos podría afectar negativamente las libertades o reproducir desigualdades sociales.

Al paso con el que las agencias estatales y el sector privado progresan en la adopción de soluciones biométricas destinadas a satisfacer las demandas de seguridad, es solo cuestión de tiempo que los objetivos originales de identificación y verificación se amplíen para incluir la utilización de un control biométrico destinado a generar perfiles de personas. Ante esta situación, cualquier desarrollo de políticas en las que se entrecrucen la tecnología de la información con las prácticas de control debería ser sometida al control democrático, al carácter firme de la normativa y a una estrecha vigilancia. De hecho, es necesario y urgente que los políticos españoles y los de la UE sean pioneros en promulgar una legislación que regule la forma de recoger, almacenar, acceder y utilizar los datos biométricos dentro del marco general europeo del "Código Deontológico de la Informática" (FIP). Las siguientes preocupaciones y recomendaciones explican las funciones exclusivas de los sistemas biométricos.

En primer lugar, los sistemas biométricos interactúan fácilmente con la tecnología de las bases de datos, lo que facilita las violaciones de la privacidad y la difusión de datos personales sin autorización, además de hacerlas más perjudiciales. Los políticos tienen que prestar mayor atención a las formas en que los datos se vinculan con identificadores biométricos y a cuál es la mejor forma de impedir que se almacenen datos personales de forma "secreta".

En segundo lugar, las tecnologías biométricas permitirán con el tiempo realizar un rastreo generalizado, lo que implica la posibilidad de vigilar los movimientos y acciones de una persona en tiempo real o de consultar bases de datos en las que se incluya información acerca de estas acciones. La Cumbre Mundial de la ONU sobre la Sociedad de la Información, celebrada en Ginebra el 10 de diciembre de 2003, puso de manifiesto el potencial y los problemas de estos sistemas obligando a los asistentes a llevar insignias de seguridad, aunque no se les informó de que contenían tarjetas inteligentes integradas y también un sistema de Identificación por Radiofrecuencia (RFID), mediante el cual se podían seguir sus pasos por toda la Cumbre. Los legisladores tienen que adoptar medidas firmes para garantizar que los sistemas de control biométrico y las bases de datos con las que se vinculan sean transparentes para las personas registradas y estén abiertos a organismos de supervisión independientes.

En tercer lugar, la identificación biométrica solo es válida si lo es también el proceso inicial de registro. Si, para empezar, una persona utiliza documentos falsos para identificarse, todas las capturas de datos relativas a esa persona en el futuro darán como resultado validaciones falsas, que supondrían un elevado riesgo para la seguridad. Es absolutamente necesario que los legisladores y los administradores de sistemas garanticen que únicamente obtienen información biométrica precisa y actualizada de personas registradas que han dado su acuerdo para tal fin con el único objeto de ser identificados y verificados.

En cuatro lugar, como quiera que los sistemas biométricos conllevan procesos de control repetidos, para los cuales se necesita no sólo una captura inicial de datos biométricos, sino capturas indefinidas en el tiempo, el "rastro de datos" que deja tras de sí una persona a lo largo de su vida se convierte en una fuente importante de información y, lo que es peor aún, en una forma de autodivulgación de la información. El principal problema que plantea la "captura longitudinal y crónica" de datos biométricos es que las personas no pueden controlar el momento en que se les introduce en el sistema, el momento en que se les rastrea, la forma en que se les incluye dentro de una categoría y para qué fines. Los legisladores deberían regular con firmeza la captura y el almacenamiento libres de datos biométricos no consentidos.

En quinto lugar, otra serie de riesgos potenciales dependen del nivel de normalización o interoperabilidad que hacen posible vincular datos entre bases de datos dispares, y esto ha de constituir un objetivo clave del fortalecimiento de la ley. Al llegar a conectar "múltiples transacciones gubernamentales, empresariales y de ocio cotidianas", los sistemas biométricos del futuro harán que sea posible reunir un "perfil completo" de los modelos de comportamiento de una persona, y esto abrirá la veda a nuevas formas de discriminación. ¿Se informará a los participantes en el programa acerca de la ampliación de los objetivos de recoger información, y de ser así, dispondrán del derecho a someter de nuevo a evaluación su participación? Es necesario limitar, mediante nuevas leyes y el fortalecimiento estricto de las mismas, la capacidad de los gobiernos (y la del sector privado) para "explotar" y reunir datos personales, excepto en los casos en los que la justicia autorice expresamente a ello para llevar a cabo investigaciones penales.

En sexto lugar, la eficacia de cualquier sistema biométrico reside en comparar datos biométricos con plantillas previamente almacenadas en una base de datos. Sin embargo, las capturas de datos de Información Personal Identificable (PII) a gran escala son susceptibles de generar una utilización malintencionada de las bases de datos. Las bases de datos y los canales

empleados para compartir datos PII son objetivos potenciales de ataques cibernéticos, robo y utilización fraudulenta. Las peticiones de datos PII que puedan realizar otras agencias y gobiernos ajenos a la UE también pueden poner en peligro la integridad de los sistemas de datos personales y debilitar la confianza de los ciudadanos en el Estado. Con respecto al sistema SIS y a su segunda generación (SIS II), un boletín publicado por la Comisión de Libertades y Derechos de los Ciudadanos, Justicia y Asuntos Interiores, reconoce que "han aparecido muchos problemas de seguridad del sistema con respecto a intrusiones y carencia de protección de datos". La UE y sus Estados miembros tienen que fortalecer las bases de datos biométricas y las redes por las que transitan los datos, además de controlar estrictamente el acceso a las mismas.

Por último, otro motivo de preocupación es la capacidad que tienen los sistemas biométricos para rastrear y crear perfiles, concretamente cuando se emplean junto con microchips RFID. Las técnicas de identificación biométrica aumentan significativamente el potencial para localizar y seguir el rastro físico de las personas y enlazar identidades individuales con modelos de consumo, historiales sanitarios y otros datos de carácter personal. La cuestión del rastreo es relevante en tanto que los sistemas biométricos prometen una elevada precisión, gran eficiencia y una amplia interoperabilidad a un bajo coste. Y es imposible que ello no traiga como consecuencia la adopción generalizada de la biometría en ámbitos públicos y privados que antes no estaban conectados, con la consiguiente multiplicación de puntos de rastreo potenciales. La utilización generalizada de la biometría para rastrear y crear perfiles podría tener como consecuencia:

• Aumentar la visibilidad del comportamiento de una persona y hacer posible la comparación del comportamiento de una persona con modelos predefinidos para obtener sospechosos o crear nuevas formas de clasificación de las personas.

• Exponer a las personas a revelaciones políticas perjudiciales o a difamación, a chantaje, e incluso a extorsión, vulnerando así la democracia y la transparencia.

• Expandir la gama de pruebas circunstanciales disponibles para la persecución penal, lo que aumenta exageradamente las posibilidades de emitir sentencias erróneas (aunque los defensores de la biometría señalan que se mejoraría la capacidad de rastrear a un sospechoso hasta la escena del delito).

• Contribuir a reprimir a personas fácilmente localizables y rastreables, dando así poder a la justicia y las grandes empresas para tratar con mano dura a personas "problemáticas" (como competidores, legisladores, líderes sindicales, denunciadores, manifestantes y activistas, clientes y candidatos políticos).

Los políticos deberán fijar un nuevo conjunto de reglamentos estrictos destinados a impedir que la tecnología biométrica de lugar a nuevas formas de discriminación y a la creación de perfiles del carácter o del comportamiento de las personas. Los administradores y controladores de la biometría deberían ser supervisados de cerca por autoridades independientes que garanticen el cumplimiento de estos principios y de las políticas relacionadas. Y lo que es más importante, la ampliación del alcance y objetivo(s) de la arquitectura general de los sistemas biométricos tiene que pasar por una revisión y una divulgación pública, además de someterse a debate *antes* de que se diseñen los nuevos programas relativos a la biometría y se construyan las infraestructuras que les sirvan de apoyo.

Conclusión: Los modos de comunicación y de control digitales y electrónicos en las sociedades avanzadas abren nuevas puertas para la vigilancia por parte de entidades públicas y privadas para fines múltiples. Las formas en que estos medios de control diversos nos prestan servicios son muy variadas y todas ellas comparten la finalidad de hacer que nuestras vidas sean más cómodas, eficientes y seguras. Los sistemas de identificación biométrica forman parte de esta extensa "sociedad del control" cuyos flujos de datos ya no se circunscriben a las fronteras de cada país. En un momento en el que los datos personales que circulan por la red se entrecruzan con los mercados internacionales y las organizaciones supranacionales, se necesita responder a cuestiones importantes sobre el poder, la ciudadanía y los progresos tecnológicos a medida que analizamos las políticas y reglamentos en materia de información para proteger a las personas de violaciones de su privacidad y de nuevas formas de categorización discriminatoria.

Afortunadamente, por el momento no es posible lograr un rastreo perfecto, pero los últimos progresos en biotecnología y en ciencia de la información, unidos a los nuevos retos en materia de seguridad, apuntan en esa dirección. No obstante, incluso la aproximación a un rastreo perfecto, sería tan "hostil" para las sociedades libres como lo sería el control sobre la innovación cultural o científica y sobre la expresión política. El nivel de riesgo general asociado con la adopción e interoperabilidad generalizadas de los sistemas de control biométrico dependen por tanto del diseño del sistema y de la voluntad política para financiar y hacer respetar una supervisión estricta del mismo. Los sistemas biométricos disponen de numerosos componentes, por lo que únicamente analizando el sistema en su conjunto podemos empezar a ser conscientes del amplio abanico de beneficios y riesgos que conlleva.

Se ha dedicado mucha atención a aplicar la biometría a la seguridad fronteriza y a la lucha contra la falsificación de documentos, en gran parte debido a que los extranjeros, los delincuentes y los terroristas constituyen un blanco fácil, en términos políticos. Como ha demostrado este análisis, la utilización de la biometría está extendiendo con celeridad sus alas. Antes de que los Gobiernos continúen ampliando sus compromisos para con los sistemas biométricos, es preciso que se

produzca una toma de conciencia pública y se celebren debates en torno a estos progresos sin parangón.

James C. Ross, Ph.D.

Subir ▲